



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,975	04/02/2004	Narasimhan Sundararajan	MS#305305.01 (5228)	1693
38779	7590	12/18/2007	EXAMINER	
SENNIGER POWERS (MSFT)			SAN JUAN, MARTIN JERIKO P	
ONE METROPOLITAN SQUARE, 16TH FLOOR				
ST. LOUIS, MO 63102			ART UNIT	PAPER NUMBER
			2132	
			NOTIFICATION DATE	DELIVERY MODE
			12/18/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/816,975	SUNDARARAJAN, NARASIMHAN
	Examiner	Art Unit
	Martin Jeriko P. San Juan	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 28 September 2007.
- 2a) This action is **FINAL**.      2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-5,7-13 and 15-20 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-5,7-13 and 15-20 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 02 April 2004 is/are: a) accepted or b) objected to by the Examiner.
 

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____.	6) <input type="checkbox"/> Other: _____.

## DETAILED ACTION

This is a response to Applicant's Amendments filed on September 28, 2007.

Claims 1-20 were originally pending.

Claims 1, 9, 17, and 20 have been amended. Claims 6 and 14 have been cancelled.

Claims 1-5, 7-13, and 15-20 are currently pending.

### ***Response to Arguments***

1. Applicant's arguments filed on September 28 have been fully considered but they are not persuasive.

Applicant argues that Wray teaches away from the Applicant's embodiment of the Applicant's invention that specifically uses the popular Simple Mail Transport Protocol (SMTP) to authenticate the exchange of public information between clients.

Furthermore, Wray does not disclose or suggest using an e-mail message for authenticating a digital object. Wray teaches away from the embodiments of the invention by specifying that the "protocol PDUs are passed between the parties operating the protocol in the form of electronic documents formatted according to self-describing markup language."

The Examiner respectfully disagrees. Wray discloses a TCP/IP connection in his invention as cited in US 2001/0010076 A1, Pg 1, Par 0024. Based on Figure 13, Wray teaches e-mails among his application services. SMTP is evident because it is the standard application layer transfer protocol used for e-mail services for all networks utilizing a TCP/IP connection. XML is a general-purpose markup language and is used by Wray to facilitate in the formatting of the data structure of protocol data units being passed in the form of electronic XML documents across various transfer protocols including SMTP [US 2001/0010076 A1, Pg 10, Par 0151]. In this regard, the protocol PDUs being "passed between the parties operating in the form of electronic documents formatted according to a self-describing markup language" does not teach away from the embodiment of the Applicant's invention using SMTP.

Wray teaches each and every aspect of the Applicant's claims described in the Prior Art rejection section. With regard to the Applicant's concern about Wray failing to disclose certain limitations described in the Applicant's Remarks, an elaboration of how the limitations are taught has been provided.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claim 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Wray [US Pub 2001/0010076 A1].

a. Based on claim 1, Wray teaches a method for authenticating the sender of a digital object, comprising: generating a first unique identifier (UID) [Alice is generating  $g^a$  where  $a$  is a random number. Par 0056-0057 and Par 0068]; transmitting from a first client to a previously known address of a second client, via an electronic mail protocol, a first message comprising the first UID [Alice is transmitting  $g^a$ . Fig 5], wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP) [Examiner notes that the client/server (Fig 1, Itms 11 and 13) read on "mail client/server" operating the SMTP.]; receiving from the second client, via the electronic mail protocol, a second e-mail message directed to the first client comprising a second UID and a copy of the first UID [Alice is receiving  $g^b$  and  $SIG_b$ . Examiner notes that  $SIG_b$  containing a signed copy of  $g^a$  reads on "a copy of the first UID." Par 0061]; and verifying the copy of the first UID is identical to the first UID at the first client [US 2001/0010076, Fig 5 – Examiner notes that Alice is verifying contents of  $SIG_b$  with her own  $g^a$  by means of computing  $g^{ab}$  (also US 2001/0010076 A1, Pg 4, Par 0066) reads on "verifying the copy of the first UID being identical to the first UID at the first client."]; and transmitting from the first client to the previously known address of the second client, via the electronic mail protocol, a third e-mail

message to the second client comprising a copy of the second UID [Alice is transmitting SIG<sub>a</sub>. SIG<sub>a</sub> contains a signed copy of g<sup>b</sup>. Par 0061]; wherein at least one of the messages transmitted to the previously known address further comprises the digital object [Certificate attributes, JUST, that are linked to public keys read on digital objects. Fig 5].

- b. With regard to claim 2, Wray teaches the method of claim 1 wherein the first message further comprises the digital object. [The digital object here is the Definition of G being sent to establish the secret key of the session. Fig 5.]
- c. With regard to claim 3, Wray teaches the method of claim 1 wherein the third message further comprises the digital object. [The digital object here is a Certificate attribute, JUST, linked to the public key of Alice. Fig 5.]
- d. With regard to dependent claim 4, Wray teaches the method of claim 1 wherein the digital object is a public key for a cryptographic system. [Public keys are inherent in Certificate attributes being exchanged. Par 0073, Par 0032.]
- e. With regard to claim 5, Wray teaches the method of claim 4 wherein the second message further comprises a second public key for a cryptographic system. [A certificate attribute, JUST<sub>b</sub>, has also been exchanged on the second message which is linked to Bob's public key.]
- f. With regard to claim 7, Wray teaches the method of claim 1 wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol. [Par 0159. (SSL protocol has recently been standardized as the TLS. Par 0002)]

g. With regard to dependent claim 8, Wray teaches the method of claim 1 wherein the first UID contains at least 128 bits. [It is inherent that the first UID be at least 128 bits to meet ANSI X9.42 standard draft for Diffie Hellman key exchange protocol.]

h. Based on claim 9, Wray teaches the method for authenticating the sender of a digital object, comprising: receiving from a first client, via an electronic mail protocol, a first electronic mail (e-mail) message comprising a first unique identifier (UID) [Bob receiving  $g^a$ . Fig 5], wherein the electronic mail protocol comprises a mail server operating the Simple Mail transport Protocol (SMTP) [Examiner notes that the client/server (Fig 1, Itms 11 and 13) read on mail client/server operating the SMTP.]; generating a second UID at a second client [Bob generating  $g^b$  where b is a random number. Par 0056]; transmitting from the second client to a previously known address of the first client, via the electronic mail protocol, a second e-mail message comprising the second UID and a copy of the first UID [Bob transmits  $g^b$  and  $SIG_b$ . Examiner notes  $SIG_b$  containing a signed copy of  $g^a$  reads on "a copy of the first UID." Par 0061]; and receiving from the second client, via the electronic mail protocol, a third e-mail message comprising a copy of the second UID [Bob receiving  $SIG_a$ .  $SIG_a$  contains a signed copy of  $g^b$ . Par 0061]; wherein at least one of the messages received further comprises the digital object.

- i. With regard to claim 10, Wray teaches the method of claim 9 wherein the first message further comprises the digital object. [The digital object here is the Definition of G being sent to establish the secret key of the session. Fig 5.]
- j. With regard to claim 11, Wray teaches the method of claim 9 wherein the third message further comprises the digital object. [The digital object is a Certificate attribute, JUST<sub>A</sub> linked to a public key of the sender. Fig 5.]
- k. With regard to claim 12, Wray teaches the method of claim 9 wherein the digital object is a public key for a cryptographic system. [Public keys are inherent in Certificate attributes being exchanged. (Par 0032)]
- l. With regard to claim 13, Wray teaches the method of claim 12 wherein the second electronic mail message further comprises a second public key for a cryptographic system. [A certificate attribute, JUST<sub>b</sub> has been exchanged on the second message which is linked to a public key.]
- m. With regard to claim 15, Wray teaches the method of claim 9 wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol. [Par 0159. (SSL protocol has recently been standardized as the TLS. Par 0002)]
- a. With regard to dependent claim 16, Wray teaches the method of claim 9 wherein the first UID contains at least 128 bits. [It is inherent that the first UID be at least 128 bits to meet ANSI X9.42 standard draft for Diffie Hellman key exchange protocol.]

- n. With regard to claims 17, and 20, these claims are rejected as applied to the like elements of claim 1.
- o. With regard to claims 18, and 19, these claims are rejected as applied to the like elements of claims 4 and 5 respectively.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan  
Examiner. Art Unit 2132

*Gilberto Barron Jr*  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100